PERFORMANCE WORK STATEMENT
For
Defense Manpower Data Center (DMDC)
Personnel Security/Assurance (PSA) Sustainment Support II

Contract Vehicle: GSA Alliant Large Business
Contract Type: Firm Fixed Price

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC), Personnel Security/Assurance Division (PSA) is seeking experienced professional information technology (IT) services to support its technology governance and customer development, sustainment and operational activities, across the software development life cycles. These services will be performed both onsite DMDC locations and offsite.

2.0 BACKGROUND

DMDC is part of a Department of Defense (DoD) Field Activity, the Defense Human Resources Activity (DHRA) which supports major programs and initiatives within the DoD. DMDC maintains the central and authoritative store of personnel, manpower, training, and security data for the DoD. DMDC is a geographically separated organization with personnel and facilities located in Alexandria, Virginia; Seaside, California; Boyers, Pennsylvania; Korea; Southwest Asia; and, Germany. While being geographically dispersed, DMDC takes pride in delivering timely and quality support to the DoD and its members. DMDC adds value by ensuring data received from a variety of sources is consistent, accurate, and appropriate when used to respond to inquiries.

DMDC quickly responds to initiatives and informational needs of DoD senior leadership which supports decision-making for a wide variety of organizations. DMDC operates major programs affecting individual members of the DoD, as well as other Federal Departments and Agencies. The programs support Active Duty, Reserve, Guard, and retired military members and their families, as well as civilian and contractor employees of the DoD. These programs include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD systems; conducting personnel surveys; performing longitudinal and statistical analyses; developing military selection, classification, and language proficiency tests; and assisting military members and their spouses with quality of life issues and transition to civilian life.

DMDC supports major programs and initiatives within the DoD and maintains the Defense Enrollment Eligibility Reporting System (DEERS), the largest archive of personnel, manpower, training, security and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970's, covering all Uniformed Services, all components of the Total Force (Active, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data on the Uniformed Services. These data support decision-making by the Office of the Secretary of Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD.

2.1 PSA SYSTEMS

On January 15, 2009, the Deputy Secretary of Defense directed that the Department strengthen and refocus the Defense Security Service (DSS) to meet 21st century industrial security and counterintelligence needs. Pursuant to this recommendation, DSS was directed to transfer "DoD enterprise wide IT systems associated with personnel security clearances to the Defense Manpower Data Center." A Memorandum of Agreement between DSS and DMDC was signed on February 2, 2010, which set forth the terms and conditions for the transfer. The transitioned systems included the Defense Central Index of Investigations (DCII); the Joint Personnel Adjudication System (JPAS); improved Investigative Records Repository (iIRR), and the Secure Web Fingerprint Transmission (SWFT). The Defense Information System for Security (DISS), including Case Adjudication Tracking System (CATS) and Joint Verification System (JVS), transitioned to DMDC effective October 1, 2015. These named applications will be known as PSA Applications. The servers for the PSA applications are located at the DMDC in Seaside, CA (iIRR is located in Boyers, PA), and the DISA Data Center in Columbus, OH.

2.1.1 JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

JPAS is a repository and centralized processing tool that provides the capability to perform comprehensive personnel security management of all DoD employees, military personnel, civilians and DoD contractors. JPAS consists of two sub-applications:

- The Joint Adjudication Management System (JAMS) - The JAMS sub-application records the eligibility determinations and unclassified investigation comments, supports the adjudication process, and automates security information records. JAMS is a system designed for the Clearance Adjudication Facilities (CAFs).
- The Joint Clearance and Access Verification System (JCAVS) - The JCAVS sub-application enables DoD Security Managers and officers the ability to view current eligibility information. It also provides the ability to update Personnel Security Information and security history.

NOTE: Operations and Maintenance support for JPAS shall continue through September 2020, at which time JPAS will be decommissioned. The decommissioning date for JPAS has been moved to September 2020 vice the original date of September 2018.

2.1.2 SECURE WEB FINGERPRINT TRANSMISSION (SWFT)

The Secure Web Fingerprint Transmission (SWFT) is a Department of Defense (DoD) enterprise system for centralized collection and distribution of electronic fingerprints for applicants requiring a background check. SWFT provides the means for collecting biometric data for personnel only once, and then reusing and sharing the data with designated DoD agencies. SWFT eliminates the need for paper-based capture and handling of fingerprints, expedites the background check process by reducing invalid fingerprint submissions, provides end-to-end accountability for sensitive PII data, and implements stringent security standards. The SWFT system consists of two major components:

- System for web-based enrollment of fingerprints (Web Enroll), which is a licensed COTS product.
- Store-and-forward system for collection and distribution of electronic fingerprint files (SWFT), which is a GOTS product.

This integrated system is also known as SWFT Plus Enrollment or SWFT+.

2.1.3 DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII)

DCII is an automated central index that identifies investigations conducted by DoD investigative agencies, and personnel security determinations made by DoD adjudicative authorities. DCII is operated and maintained on behalf of the DoD Components and Office of the Deputy Under Secretary of Defense for Human Intelligence (HUMINT), Counterintelligence and Security. Access to DCII is normally limited to the DoD and other federal agencies that have adjudicative, investigative and/or counterintelligence missions.

2.1.4 improved INVESTIGATIVE RECORDS REPOSITORY (iIRR)

iIRR is a repository for the legacy subject records of any personnel security investigation opened and closed within the DSS' Case Control Management System – Information System (CCMS-IS) prior to its decommissioning on 3 February 2006. Some of the investigative records are stored electronically and some files are on microfiche. The iIRR access is restricted to a team of DMDC staff on a closed network due to the sensitive nature of the investigative records.

2.1.5 DEFENSE INFORMATION SYSTEM FOR SECURITY (DISS)

DISS was developed in response to the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 and the Joint Security and Suitability Reform Team (JRT) focus areas to improve the federal security and suitability clearance process. This new process was outlined by the JRT in the April 2008 Initial Report on Security and Suitability Process Reform, which provided a framework for an enterprise-wide, end-to-end process supported by appropriate IT systems to make hiring, credentialing, and clearance processes meet IRTPA guidelines on efficiency and timeliness.

The Office of the Under Secretary of Defense for Intelligence (OUSD(I)) is the functional sponsor and has established and defined the top level operational requirements for DISS. The DISS solution will support information sharing between various DoD entities, as well as among a number of other federal agencies. It will be managed and maintained by the DISS PMO. The DISS PMO will follow guidance of, and escalate issues to, the appropriate DISS Governance Board.

DISS will replace various security clearance and suitability systems, enabling an enterprise solution with consistent standards and reciprocal recognition for all DoD security clearances and suitability/fitness for employment determinations. The DISS program focuses on solutions for three of the reform areas:

- Validate Need – DISS is working with Office of the Director of National Intelligence (ODNI) and the Office of Personnel Management (OPM) to create a federated search capability to support reciprocity and reduce unnecessary duplicate investigation and adjudicative processes.
- Electronic Adjudication (e-Adjudication) – DISS employs technology to apply business rules and render security, suitability, and credentialing adjudication decisions electronically in cases with no actionable issues.
- Continuous Evaluation – Support the Automated Records Check workflow so records for existing cleared personnel can be analyzed more often to flag potential concerns.

Enhancing these primary areas of the reform security and suitability processes will allow the DISS program to improve timeliness, reciprocity, quality, and cost efficiencies through the design and implementation of a secure, end-to-end IT solution.

- Case Adjudication Tracking System (CATS) - CATS supports the process of rendering applicant's eligibility determinations for a security clearance, suitability or fitness for employment, and credentials by providing a framework for assessing an applicant's trustworthiness and fitness. To date, CATS is successfully implemented at the Army CAF, Navy CAF, DISCO, Washington Headquarter Services (WHS), and Air Force CAF. These implementations have already achieved substantial improvement in the overall time necessary to adjudicate clearances. CATS will be consolidated into a single, enterprise version within DISS. CATS is replacement for the JAMS sub-application in JPAS.
- Joint Verification System (JVS) - JVS will provide the functionality for the maintenance and verification of security, suitability, and credentialing eligibility information. JVS will support the concept of a virtual Security Management Office (SMO), providing an access point for Security

Officers to manage security information, including subject access levels and eligibility. JVS will be JPAS' JCAVS replacement.

3.0 SCOPE

The Contractor shall provide the full range of IT services, technical and management expertise, and solution-related enabling products in one or more of the functional categories to meet the mission needs of the DMDC for PSA Applications (JPAS, SWFT, DCII, iIRR, and DISS). The contractor shall adhere to the performance standards in this contract as well as industry accepted best practices where such does not conflict with the requirements specified while utilizing all proposed innovative solutions and cost savings initiatives. As identified in individual tasks, information technology solutions/capabilities will support DMDC on a world-wide basis. The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and any other items or resources to perform this scope of work, including non-personal services necessary to deliver sustainment and operational support activities as defined in this Performance Work Statement (PWS) except for where required by the Government as specified in the PWS.

Services provided under this task order shall include Project Management and Software Development Life Cycle (SDLC) requirements. The specific depth and breadth of the activities will vary over the implementation of the project, and include requirements definition, functional and technical specifications, design, project planning, development, testing, and implementation. With the pace of change, it is impossible to anticipate how IT requirements and programs will evolve over the life of the contracts. These services represent a broad set of contemplated work requirements and must not be construed as the only activities to be to be performed on this task order.

The Contractor will work closely with various divisions within DMDC, and other agencies to ensure the success of each application. To achieve success the contractor shall have a complete understanding of DMDC's system infrastructure, configurations, tools, and components.

4.0 REQUIRED TASKS

4.1 PROGRAM MANAGEMENT SUPPORT

4.1.1 Project Management

The Contractor shall provide management and oversight of all activities performed by Contractor personnel, including subcontractors, to meet the requirements identified in this PWS.
The Contractor shall provide program management support under this Task Order utilizing industry best project management practices (Project Management Body of Knowledge (PMBOK®) Guide), which include all of the tasks required to initiate, plan, manage, control, report and close-out this task order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors/teaming partners, to satisfy the requirements identified in this Performance Work Statement (PWS).

The Contractor shall document their approach in a Project Management Plan (PMP). The initial draft PMP shall be submitted in accordance with (IAW) the Deliverables Schedule in Section 7.1. The PMP shall describe the Contractor's management approach, operating procedures, support priorities, service levels, and estimated staffing. The PMP shall include an overall WBS and associated responsibilities and partnerships between Government organizations. The PMP shall show milestones and tasks for short term and long term projects. The PMP shall, at a minimum, address:

- Process management and control (i.e. monitoring mechanisms, program metrics)
- Personnel management to include coverage and organizational structure
- Financial management to include cost containment and cost forecasting
- Technical Effectiveness to include routine Operation and Maintenance (O&M) and implementation and integration of new hardware and software, and technical refresh procedures
- Operational effectiveness to include system administration, account management, implementation of new hardware and software, and technical refresh procedures
- Quality Control Plan (QCP)
- The PMP shall include establishment of task support in relation to incrementally provided funding IAW customer established task priorities.

The Contractor shall provide the Government with a draft PMP, on which the Government will make comments. The final PMP shall incorporate Government comments. The Contractor shall keep the PMP up-to-date IAW with the Deliverables table (Section 7.1)

4.1.2 Orientation Briefing

Within two weeks of award, the Contractor shall conduct an orientation briefing for the Government, inclusive of DMDC and GSA personnel. The Government does not want an elaborate orientation briefing nor does it expect the Contractor to expend significant resources in preparation for this briefing. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the following:

a) Introduction of both Contractor and Government personnel performing work under this Task Order.
b) The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this PWS.

The Contractor shall provide two (2) hard copies of their proposal (technical and price) to the Government at award.

4.1.3 Transition Plan

The Task Order transition-in and ramp-up period is expected to begin from date of award and will be phase-in with full performance beginning NLT 15 Oct 2017. The transition plan shall be delivered NLT the scheduled contract kick-off meeting. The Contractor shall begin transition-in activities immediately after task order award.

The contractor shall develop an outgoing transition plan (Deliverable 4) to provide a detailed transition strategy/plan from their own support to another contractor. The outgoing transition plan shall be due 90 days prior to task order completion.

The transition plan~~s~~ at a minimum shall include: participating in the planning and transition of the applications during the period of performance; provide a communication plan which details the transition plans and schedule with all stakeholders; provide detailed briefings regarding the structure of the database tables, software required continuing maintenance, and operation of systems developed under this contract; transfer all project materials (source code, documentations, etc.) to the successor Contractor upon direction from the Contracting Officer and in a manner prescribed by the Government. The transfer shall be completed by the expiration date of the contract and shall include provision by the incumbent Contractor of accurate and complete data files and pertinent documentation.

4.1.4 Meetings

Participate in the initial "kick off" meeting: This meeting shall be conducted within the first ten (10) business days after contract award.

Participate in bi-monthly status meeting: The purpose of this meeting is for coordination and information sharing with other DMDC. This meeting should contain all initiative statuses (e.g. status, timelines, risks, issues, etc.), open DMDC/stakeholder's ad hoc reports, recommendations, and any other necessary information that the Government needs to be aware of.

The deliverable (electronic and hard copy) shall be the following:

- Provide meeting minutes to DMDC COR within five (5) business days

4.1.5 Senior Management Reviews (SMR)

Participate in SMR Reports (see Appendix E for acceptable sample format). An SMR report shall be submitted every 15th of each month. The monthly SMR report shall summarize the following information:

- accomplishments during the period,
- problems met or anticipated,
- activities anticipated during the next reporting period,

These reports shall be submitted to the Contracting Officer's Representative (COR) by e-mail and in GSA ITSS system. Each monthly SMR report shall be submitted by the 15th business day of the month following the period reported upon.

4.1.6 In-Progress Review (IPR)

In addition to the specific deliverables and associated reviews listed, the contractor shall schedule, organize and present In-Progress Reviews (IPRs), not less than bi-annually (preferably quarterly), during the period of performance of this task order. The method of presentation shall be in the contractor's project management plan. The objectives of these reviews are to track progress of the project, present ideas for improvement, and identify and resolve issues. The contractor shall coordinate the requirements of the IPR with the DMDC Technical Representatives and COR.

4.1.7 Quality Control Plan

Produce a Quality Control Plan (QCP) which will be used as the contractor's internal plan to insure delivery of quality products and services under the terms of the contract. The QCP shall detail the contractor's internal controls for services under this contract and shall have a direct relationship to the proposed terms of the Performance Requirements Summary (PRS), see Appendix A. The outline for the QCP shall be submitted ten (10) days after project "kickoff" meeting. The completed QCP shall be delivered forty-five (45) calendar days after award.

4.1.8 Problem Notification Reports

Notify the DMDC COR, GSA COR and GSA Contracting Officer of any problems or potential problems affecting performance. Verbal reports of problems shall be followed up with written reports within ten (10) calendar days.

4.2 SUSTAINMENT AND OPERATIONAL SUPPORT OF PSA APPLICATIONS

The contractor shall provide sustainment and operational support for all identified PSA Applications. This includes the Joint Personnel Adjudication System (JPAS); the Secure Web Fingerprint Transmission (SWFT); the Defense Central Index of Investigations (DCII); the improved Investigative Records Repository (iIRR); and the Defense Information System for Security (DISS).

All PSA applications with the exception of DISS and JPAS are fully integrated in the standard DMDC environment. The JPAS and DISS application support will be from the Operating System (OS) up. The SWFT application support will be also from the Operating System (OS) on up, with the exclusion of the data tier. If a task is for a specific application, it will be noted as such. iIRR Production environment is not in the standard DMDC environment. iIRR is located on a standalone, air-gapped enclave at the customer site in Boyers, PA.

The contractor shall provide ongoing sustainment, operational and production level support for the PSA applications within the production, pre-production, failover, development, and test environments and ensuring all aspects of the applications, including any reports, continue to function at the efficiency and capability levels intended as detailed in Appendix B “Guidelines and Parameters for Resolving System Problems”, and Appendix C “System Outage Notification Procedures”. This effort will require support for each of the technologies used for the applications.

- For JPAS DISS: The development environment will be maintained in the vendor location. The goal for DISS will be to transition from the development vendor location to a DMDC or specified DoD environment.

The contractor shall detect all outage/issue/problems that adversely affect the performance and/or vulnerability of the systems and work with DMDC Systems to assist to resolve the outage/issue/problem, and notify the Government/stakeholders, as defined by DMDC, as soon as possible even prior to the resolution in accordance with Appendix B & C.

- For JPAS, DISS and SWFT: In addition, the contractor shall have a proactive approach by utilizing automated system-monitoring techniques to identifying recurring problems, reporting to the Government those problems, and recommending solutions to mitigate recurring problems of the same nature. Resolve all outage/issue/problems from the OS level on up. Work with Systems to resolve all outage/issue/problems on the OS level.

The contractor shall provide support by assisting in identifying and resolving application system problems and/or vulnerabilities. This includes recommendations, consultations, coordination, evaluation, testing and deployment to resolve.

- For JPAS, SWFT, and DISS: In addition, the contractor shall identify and resolve application system problems and/or vulnerabilities from the OS level on up.

The contractor shall provide database administration services that shall perform modifications to the PSA applications while maintaining continuity of the data to include performing schema changes and conversion of the production database during application upgrades and new version releases.

- For JPAS, DISS and SWFT: This will be administration from the OS on up. For all other PSA applications, this is at the application database level.

- For JPAS and DISS: The contractor shall maintain database replication between all backup site locations and all server replicates.

The contractor shall provide support, maintain, and keep the test, development, and pre-production PSA applications consistent with current application upgrades and new version releases, while providing database refreshment of all database instances. Ensure that all data used in these environments follow DMDC's Personal Identifiable Information (PII) Policies. Data will need to be refreshed at the request of the PM or at least once a year.

- For JPAS, SWFT, and DISS: The contractor shall support, maintain, and keep the test, development, and pre-production PSA environment consistent with current application upgrades and new version releases, while providing data refresh on all database instances.
- For JPAS and DISS: The contractor shall build out the necessary environment(s) to allow for the PII to be removed and to be used to replace the PII environments that are currently being used by the data team. Some work will be dependent on another contractor.

The contractor shall assist in failover planning, testing, and execution at least once a year and during any major outage where when the Government deemed failover necessary.

- For JPAS, SWFT, and DISS: The contractor shall conduct failover planning, testing, and execution at least once a year and during any major outage when the Government deemed failover necessary.

The contractor shall modify the applications in accordance with Change Requests (CRs) and Problem Reports (PRs) approved by the DMDC Technical Representative (TR).

The contractor shall collaborate with PSA system's partnering agencies (e.g., OPM, DSS, Armed Services, Accessions, Industry) to maintain fully functional interfaces, process data; resolve data and/or technical issues; and/or update the interfaces when needed. This includes decommissioning of interfaces when no longer needed and updating the interfaces as the partnering agency transition over to the new ISO country codes, if applicable.

The contractor shall ensure that quality assurance requirements are enforced for all aspects of the software revision process. This includes collecting and analyzing quality metrics, performing detailed reviews, walkthroughs, requirement traceability analyses, defined verification and validation processes that occur during the course of software maintenance to ensure that requirements are traceable, consistent, complete, and successfully tested. The contractor shall ensure the software correctly reflects the documented requirements which include conducting, reporting on, and/or participating in formal reviews, informal reviews, inspections, peer reviews, tests, and evaluations to ensure the code meets operational and security requirements and does not negatively impact performance of the system.

For iIRR: The contractor shall provide production system stand-up support and isolated environment application modifications.

- The contractor shall ensure the modified Production system operates within DMDC Boyers' isolated environment. The Contractor shall be responsible for sustainment tasks including defect fixes, defect tracking, delivery of fixes, application code modifications to support hardware, configuration, and/or network changes, updates to guides and design documentation.
- The contractor shall provide full Production Support for future releases and deployments to include delivery and configuration of application, configuration of Weblogic parameters,

configuration of LDAP schema and user groups, configuration of additional dependent COTS software.

4.3 CUSTOMER, DATA, AND FIELD SUPPORT

The contractor shall maintain and ensure data accuracy and data integrity. The contractor shall analyze and resolve data errors/issues/problems and resolve. If any data integrity/error/issue with a record is identified, the record shall be updated/corrected within fourteen (14) business days or within timeline specified/agreed upon by the PSA Application PM, and the resolution will be communicated to the Government, stakeholder, customer, and/or interface. If the source of the problem originates from an interface, communication to the data source/interface must be made within 48 hours of discovery to include identification and recommendation to for problem resolution. This coordination with external interface owners/customers for data correction also includes periodic and timely follow-ups until data issue is resolved.

Data quality assurance team to ensure data conforms to data standards. This task may include performing quality control checks to JPAS and DISS data, verifying scripts, correcting data and ensuring data is meeting standards set by the Government to ensure that JPAS and DISS data will not only meet data quality standards but also be able to be migrated.

The contractor shall add, create, modify, or delete super users/Non-DOD/special circumstances user accounts or settings within three (3) business days of notification unless immediate add/modification/removal is needed.

The contractor shall create and provide customized reports or data extracts based on DMDC or stakeholder's requirements. Reports or data extracts shall be provided within seven (7) business days from receiving the Government's request or within timeline specified by the PSA Application PM.

The contractor shall provide review, evaluation, advice, answers and/or guidance on products or deliverables relating to the PSA Applications to the Government, Stakeholders, Call Center, and customers.

For SWFT: The contractor shall act as the point of contact between the SWFT user community and Government to coordinate and manage day to day SWFT activities. This function is generally known in the SWFT user community as the SWFT Coordinator, and includes the following responsibilities:

- Monitor and maintain the SWFT mailbox ensuring that all requests, questions, issues and other communications are addressed within two (2) business days
- Manage and coordinate the registration and approval process for fingerprint capture devices with DMDC, OPM or other entities
- Coordinate with the SWFT Administrators timely release of electronic fingerprints to their requested destinations
- Coordinate with the Call Center/Help Desk and the SWFT Administrators the resolution of issues related to the SWFT application
- Produce and maintain program documentation such as: weekly activity reports, system metrics, SWFT registration documents, and SWFT FAQ's
- Monitor, analyze, and report on processes and procedures related to the use of the SWFT system, fingerprint submissions, fingerprint submission site and fingerprint capture device registration, and make recommendations for improvement and enhancement.

For SWFT: The contractor shall act as the point of contact between the online fingerprint enrollment user community and DMDC to manage and coordinate day to day activities. This function includes the following responsibilities:

- Create and manage online enrollment system user accounts
- Create, manage and assign the enrollment user groups, sub-groups, and location profiles
- Respond to client communications and ensure that all requests, questions, issues and other communications are addressed within two (2) business days
- Coordinate with the SWFT Coordinator and Administrator timely release of electronic fingerprints
- Coordinate timely resolution of issues related to online fingerprint enrollment with the Help Desk, SWFT Administrators and SWFT application technical support
- Produce and maintain program documentation such as: weekly activity reports, system metrics, and FAQ's specific to online fingerprint enrollment
- Monitor and analyze processes and procedures related to online fingerprint enrollment subsystem usage, fingerprint submission traffic, fingerprint enrollment site, and fingerprint capture device registration, and make recommendations for improvement and enhancement.

For DISS: Act as the operational point of contact between the DISS user communities. Monitor and maintain the DISS mailbox(es) ensuring that all requests, questions, issues and other communications are addressed within two (2) business days; coordinate with the Call Center/Help Desk and the System Administrators for the resolution of issues related to the DISS applications; produce and maintain program documentation such as: weekly activity reports, system metrics, and standard operating procedure(s); monitor, analyze and report on processes and procedures related to the use of DISS application(s), and make recommendations for improvement and enhancement.

For DISS: DISS must be able to receive data from CE in order to place a new investigation on a subject's record. This will include a CE Alert Flag to identify if a CE alert is on a subject's record as well as a CE investigation history start date and end date on a subject's record. There may be multiple CE investigations, dependent on DoD affiliation. There also may be multiple CE alert flags at various times.

4.4 TESTING SUPPORT

The contractor shall develop and conduct thorough testing in the development and test environments to ensure optimum performance is maintained to include functional testing of interfaces and application changes, as defined in the Functional Test Plan, prior to releasing the software and/or IA patches for testing in the Government's pre-production environment.

- For JPAS, SWFT, and DISS: Upon completion of the contractor's initial testing and quality assurance testing, all software coding shall be tested in the Government's pre-production environment to ensure proper validation of enterprise systems and applications prior to deployment into the production environment.
- For DCII: The contractor shall conduct functional testing prior to releasing the software and or IA patches to the production environment.

The contractor shall ensure all errors identified during the tests, to include tests in the Government's pre-production environment are resolved. Once testing has been accepted by the Government, the modifications can be deployed to production.

4.5 CONFIGURATION MANAGEMENT (CM) SUPPORT

The contractor shall perform the CM activities of configuration status accounting, configuration baseline management, creating and maintaining a configuration management library system to control the release of products, manage their history, administering a change management procedure, and tool to track all CRs or PRs to the baseline as well as all issues.

The contractor shall perform the accepted and practiced DMDC CM processes in conjunction with internal and external procedures, plans, and polices of the Agency to include informing, coordinating, providing and documenting all baseline system documentation, modifications to existing and developing system(s) under the Agency's purview through the DMDC CM group. Baseline system documentation includes system designs, build procedures, requirements documents test procedures, problem reports, software code, and system knowledge base.

4.6 INFORMATION ASSURANCE (IA) SUPPORT

NOTE: For PSA Applications running in standard DMDC infrastructure, the scope of this task will be generally limited to application-level support. For JPAS, SWFT, and DISS, the scope of support is from the OS level on up.

The contractor shall perform all work within the scope of this contract in strict compliance with all applicable DoD Security Regulations and DoD Information Assurance Regulations, USCYBERCOM Orders, Federal Information Security Management Act (FISMA) and DMDC Security policies to include: maintaining the Trusted Facilities Manual and Security Features Users' Guide required by DoD, monthly IA Security Vulnerability Reports, participating in the Certification and Accreditation process, using protective tools such as Security Technical Implantation Guide (STIG), Security Readiness Reviews (SRRs) or checklist on a reoccurring basis using the appropriate tool (or other tool as defined by the Government), providing and implementing the necessary Information Assurance/Computer Network Defense (IA/CND).

The contractor shall create and adhere to procedures & guidelines which are created to comply with DoD and DMDC security policies. The contractor shall ensure that all data leaving DMDC systems in transit or at rest be protected according to DODI 8500.2. Specific policies are listed as DODD 8500.1; DODI 8500.2; DODD 8570.01-M; DODD-O-8530.1; DODD-O-8530.2; and DoD 8510.10. These policies are available at http://www.dtic.mil/whs/directives/corres/ins1.html.

The contractor shall take immediate action to assess the impact of each vulnerability, develop patching plans, provide First Report requirement, create the necessary Plan of Action and Milestones (POA&M), and test patches to ensure no negative impact. Testing shall be conducted to ensure IAVM actions will not impair system operations.

- For JPAS, SWFT and DISS: In addition to 4.1.15.3, the contractor shall patch all application software and server components accordingly while following DMDC's IA policies and regulations. IAVM compliance will be ensured through 1) the normal Certification and Accreditation (C&A) process, and 2) monthly scanning of the systems using tools used by DMDC. The results of these scans will be sent to the Information Assurance Officer (IAO), to be identified post award. This sub-task does not include SWFT.

The contractor shall support obtaining accreditation via certification testing of its respective element(s). This task will consist of process, analysis, coordination, security certification test, self-evaluation, conducting system security assessments, and security documentation support, assisting the Government in the implementation of Certification and Accreditation.

The contractor shall ensure the Information Assurance Manager (IAM) and IAO are informed on system security matters, address specific security issues, and obtain guidance.

- For JPAS and DISS: The contractor shall provide any necessary documentation (e.g. Certification and Accreditation reports, Monthly Vulnerability Reports, First Reports, POA&Ms) to DMDC's IAO.

4.7 DISS DEVELOPMENT SUPPORT (CATS AND JVS)

The contractor shall continue the development of the full set of sub-applications and services to include development of data delivery components implementing the functional and technical requirements, architecture, and all data and security services.

The contractor shall ensure proper authentication and authorization of a user based on their individual role and level are allowed proper access by using subject and security management office (SMO) data services to read data. Authentication will utilize all DOD-approved Public Keys and will utilize existing DMDC application security and operator provisioning services.

DISS application development assumptions:

- Agile development strategy to meet the emerging requirements of the user communities
- Quarterly deployment of major code releases for each DISS component with minor releases as needed to address defects, mandated updates, etc. (Total: 8 annual releases)
- Application updates due to policy changes will be prioritized for release within 60 days unless otherwise specified by the Government

The contractor shall maintain subject-related data services to create, read, update, and search for subject information.

The contractor shall maintain SMO data services to create, update, and deactivate SMOs, and manage SMO-subject relationship information and tasks.

The contractor shall maintain eligibility data services to create, read, update, and remove eligibility information for subjects.

The contractor shall maintain foreign relationship and foreign trip data services to create, read, update and delete foreign relationship and foreign trip information for subjects.

The contractor shall maintain access data services to grant, remove, suspend, and reinstate access for subjects to classified data.

The contractor shall maintain visit data services to create, validate, access, and modify visit information for a subject's visit to a facility to discuss/access classified information.

The contractor shall develop incident data services to create, update and close incidents that would impact a subject's eligibility and/or access to classified information.

The contractor shall develop notification/message data services, including support for continuous evaluation to notify users and SMOs of various activities during the operation of the system.

The contractor shall ensure, for all services that are developed, full integration with the DMDC Common Update Framework (CUF), Application Programming Interfaces (APIs), DMDC's application security and operator provisioning services, ensuring that proper transactions are maintained at all times, and shall rollback any uncommitted transactions in accordance with ACID.

The contractor shall ensure that authorized users have the ability to access all functionality of the application to include add, update/modify, delete based upon their user role and level.

The contractor shall provide systems engineering support to include the development of the software development lifecycle documents and participate in technical reviews of the documents. These including: System Requirements Document (SRD), High-Level Design Document, Low-level Design Document, and System Test Plan.

The contractor shall maintain the Extract, Transform & Load (ETL) capability to extract the Oracle JPAS data and transform it into the CUF subject model format and load the data into the DISS JVS database.

The contractor shall maintain the ETL capability to extract person and personnel data from the Oracle JPAS data store and load the data into the DMDC Person Data Repository (PDR).

The contractor shall maintain the ETL capability to extract SMO- and authorization-related data from the Oracle JPAS data store and load the data into DMDC's EMMA data store.

The contractor shall build an Archive ETL capability to extract the Oracle JPAS data (and DISS JVS Oracle), transform it into an archive format, and load it into the DISS Integrated Data Store (IDS) data warehouse.

The contractor shall develop referential integrity rules to be applied to screened data to ensure that proper relational database design integrity is applied throughout the destination database.

The contractor shall perform data migration V&V activities on JPAS and Legacy CATS data. In order to properly execute these activities, it shall be necessary for Contractor to properly execute V&V scripts using date/time segmentation. Contractor shall inspect and determine whether other segmentation strategies may be necessary to segment data using other data in the JPAS nd/or Legacy CATS database (e.g. Person, Personnel, etc).

The contractor shall fully and successfully migrate the existing JPAS data into JVS. The contractor shall fully and successfully migrate the existing legacy CATS data from the multiple versions into enterprise DISS sub-applications CATS and JVS. This includes ensuring the data is free of data errors, data conversion is complete and accurate, and all identified data errors, inconsistency, and transformations to fix anomalies/data errors are completed. This includes using the existing Sybase-to-Oracle (Vendor) ETL script to transform the data from Sybase to Oracle without changing the structure.

4.8 PSA SYSTEMS OPTIONAL SUPPORT

4.8.1 Optional Support Guidelines

The Government reserves the unilateral right to exercise the following optional services. Optional support will be invoked through award of a Task Order modification issued by the Contracting Officer. Optional services may be invoked, in whole or in part, at the discretion of the Government.

At the time of exercising optional support, the Government will further definitize requirements, where necessary to:

a. Provide technical direction necessary to clearly delineate the extent of support and nature of work to be performed, deliverables and required timeframes, if any.
b. Specify technical details about the specific environment (e.g. network, systems, applications, tools) where support is required.
c. Identify place(s) of performance.
d. Define the business hours in which support is required and specify requirements, if any, for providing coverage or recall during non-standard business hours.
e. Identify required service level(s) and performance standards, if any.
f. Specify security clearance requirements.
g. Identify specific certification requirements of DoD Manual 8570.01M, Information Assurance Workforce Improvement Program applicable to the option being invoked.
h. Identify any required Travel or ODCs (as a NTE amount).

4.8.2 Potential Optional Tasks

Options described in PWS Section 4.8.1 may be invoked to support DMDC requirements that fall within the scope of the requirements of this PWS.

Optional positions are anticipated to include technical skillsets similar to the labor mix performing mandatory services under this Task Order.

For proposal purposes, the Not-to-Exceed (NTE) value of this option is **$5,000,000.00** per year. The value of this option includes labor, ODCs, and travel support.

Examples of potential tasks and/or efforts that may impact this task order include the following, but are not limited to:

- Enhancements to PSA Applications
- NBIS architecture and design changes to DISS for enterprise case management workflow
- NBIS architecture and design changes to SWFT for enterprise fingerprint management and interfaces
- NBIS design changes to meet FOIA and Privacy Act release requirements
- NBIS application changes to CATS to support Federal adjudicative workflow and interfaces
- NBIS and/or NBIB application changes to JVS to support Federal subject management workflow and interfaces
- NBIS enterprise data repository to support Federal agency case file requirements
- Implementation of DISS and SWFT from DoD-only to multiple Federal Agencies. This will include an expansion of infrastructure, addition of data interfaces with various Federal systems, management of Federal users and subjects, as well as support services to include areas such as call center operations and Privacy Act processing.
- Integration of DISS, SWFT, and other applicable DMDC systems into a common NBIS Data Repository that will be shared with other NBIS systems. This will require modifications to the applications as well as the underlying architecture.

- Standardization and rationalization of the DISS, SWFT, and other applicable DMDC/NBIS systems as appropriate to improve integration.
- Design and development of a shared authentication and authorization component for user logon which works across the entire federal government and can be used by all of the NBIS application components.
- Integration with other OPM/DISA applications (e.g., FTS (Fingerprint Transmission System), e-App (replacement for OPM's e-QUIP, and a Case Management application).
- Increase of security controls and postures of DISS, SWFT, and other applicable DMDC systems from the infrastructure, architecture, data, and application perspectives.
- Adoption of ongoing Business Process Re-engineering by the Office of Management and Budget (OMB) Personnel Advisory Committee (PAC) for the Federal Security, Suitability and Credentialing processes.
- The design, development, and testing of new application requirements and deemed required by the NBIS Information Technology Governance Board (ITGB).
- Implementation of the DMDC applications into different NBIS environments to include but not limited to Development, Test, Production, and Disaster Recovery.
- Support full scale testing of the applications by the Joint Interoperability Test Command (JITC), and make any required application changes in response to deficiencies found during testing.
- SWFT integration with DoD and NBIS Pilot and Proof of Concept Initiatives
- DISS integration with DoD and NBIS Pilot and Prototype Initiatives
- Modification of applications due to policy changes
- Addition of interfaces
- DCII migration to PK-enabled log in
- Integrate the User Deactivation Utility into the DCII application
- Remove the SSNs from the directory paths in the iIRR Production Towers
- Streamline and improve application maintenance, testing and performance
- Migrate application code from new COTS product or version
- Modify application inputs, outputs and reporting to meet regulatory and policy compliance
- Modify design and architecture to maintain cyber security compliance
- Develop, test and deploy new CATS functionality, workflows, and procedural changes
- Develop, test and deploy new JVS functionality, workflows, and procedural changes
- Develop, test and deploy new or modified reports, standard and ad hoc report data elements
- Develop, test and deploy new web services and interfaces

4.8.3 DISS and SWFT Development Support (Optional T&M)

DISS and SWFT are DoD capabilities identified for integration into the National Background Investigation Services (NBIS) designated to replace the Office of Personnel Management (OPM) information technology in support of an end-to-end Federalized solution for national security, suitability and Personal Identify Verification (PIV) credentialing eligibility determinations. NBIS has adopted an agile development strategy and DISS/SWFT will need to leverage an agile development strategy to be able to meet the evolving requirements as defined through collaboration with NBIS, NBIB, and DoD functional sponsor for the personnel security mission. DMDC and NBIS will leverage agile best practices for software development to provide the iterative products and services that will require rapid adjustment to meet integration goals as system capabilities are delivered while allowing the continued use of these production systems. In adopting an agile development methodology (rapid development), DMDC will meet the software development lifecycle through abbreviated regular cadences or sprints.

The evolving nature of the requirements do not allow for specific contract requirements with definitive delivery dates to meet a firm fixed price contract strategy. DMDC require maximum flexibility and use of a time and materials for the development contract line item number to be able to:

- deliver interfaces with the existing DMDC and OPM system components to support transitional capabilities (e.g. eQIP, Mirador,)
- develop interfaces with new NBIS system components in parallel development cycles
- develop additional roles to meet Federal requirements (e.g. adding Executive Branch Federal Agencies)
- modify or develop additional workflows to meet Federal requirements
- integrate capabilities from existing OPM system components (e.g. CVS)
- add capabilities to meet DoD and Federal requirements
    - Add ability to view investigative documents
    - Record conditions, waivers, and exceptions
    - Streamline adjudicative workflows for manual entry of eligibility determinations
    - Develop end-to-end suitability workflow
    - Develop end-to-end insider threat workflow
    - Add Divisions and business rules for Insider Threat mission
    - Add Hierarchy and New User Roles for Federal Agencies
    - Develop operational reports
    - Add Tiered eAdjudication business rules (T1, T2, T4)
    - Add QART reporting requirements
    - Add SEAD3 self-reporting requirements
    - Add commercial identify verification

The Items to be delivered in the Base Year release cycle are:

SWFT

- Investigation Management (IM) Interface
- Mirador Interface
- Secure FTP Interface for Background Investigation (BI) Mission

DISS

- Investigation Management (IM) Interface
- Mirador Interface
- UI workflow deficiencies

The estimated Change Requests to occur in the Base Year are listed below. Support is anticipated to be needed at the same level for Option Year 1, but Change Requests are not defined at this time.

- CR492-Privacy Office Disclosure Capture
- CR489-Privacy User Interface (UI) Changes
- CR443-Privacy UI Changes to Restrict Subject Summary Tab
- CR456-Privacy UI Changes
- CR-Manual Re-assignment Permission for Adjudicator Role
- CR504 -Interim CSR w/o Advanced NAC
- CR502-Component Adjudicator record OPM/NBIB takes jurisdiction
- CR509-Priority Program Flags permission for Industry Process Team
- CR510-Add Task Date for Task Inbox
- CR516-Unclaim tasks for reassignment

- CR520-Document upload optional
- CR529-History listing subject owning or servicing relationships
- CR-Forward ROI to Component Adjudicator
- CR459-Manually push case to SMO
- CR472-Transfer tasks between SMO
- CR454-Transfer tasks between SMO
- CR474-DISS Notification of Subject Change(s)
- CR344-Display Task Owner in Task Inbox
- CR398-Add Guardian and Foster Parent as Relationship Types
- CR319-RFA generation for Industry Process Team
- CR173-Add SON and make modifiable
- CR221-Add data elements to reporting for analytics (ad-hoc) reporting
- CR222-Add data elements to reporting for analytics (ad-hoc) reporting
- CR471-Submit Multiple CSR

5 PERIOD OF PERFORMANCE

This task order consists of 12-month Base Period with four (4) subsequent 12-month option periods, with an effective date, as follows:

- Transition/Base Period: 16 Sep 2017 through 15 Sep 2018, *(Note: It is anticipated that the Transition Period will be from 15 Sep2017 through 14 Oct 2017 and fully operational performance under the base period would begin on 15 Oct 2017.)*
- Option Year 1: 16 Sep 2018 through 15 Sep 2019
- Option Year 2: 16 Sep 2019 through 15 Sep 2020
- Option Year 3: 16 Sep 2020 through 15 Sep 2021
- Option Year 4: 16 Sep 2021 through 15 Sep 2022

The Government may extend the term of this task order by written notice to the contractor within 15 days of the expiration of the existing period of performance provided that a preliminary notice of the Government's intent to extend is provided at least 30 days before the expiration of the task order. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended task order shall be considered to include this option clause. The Government shall have the unilateral right to exercise options periods.

6 PLACE OF PERFORMANCE

6.2 Location

The primary work location will be at the contractor's location(s) with some personnel in Seaside, CA at the DMDC facility. The DMDC facility in Seaside, CA can accommodate no more than 9 Full-time Equivalents (FTEs); and the DMDC facility in Alexandria, VA can accommodate no more than 2 FTE.

6.3 Hours of Operation

The contractor is responsible for conducting business, between the hours of 8 a.m. to 5 p.m. (local time), Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons.

Contractor operations support personnel shall provide pro-active monitoring of the Personnel Security and Assurance (PSA) applications and the COTS products that support them with the DMDC enclave during normal business hours (0800 to 1700 hours EST/DST, Monday to Friday). The contractor shall also have personnel available for on-call after-hours emergency support either through VPN or on-site, twenty-four hours a day, seven days a week. It is anticipated that the PSA systems will be instrumented with enterprise management and monitoring tools (e.g. BMC patrol) that can automatically alert contractor operations support personnel (via email or pager) in case of system problems.

6.4 Government Holidays

The following Government holidays are normally observed by Government personnel: New Year's Day, Martin Luther King's Birthday, Presidential Inauguration Day (metropolitan DC area only), President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, Christmas Day, and any other day designated by Federal Statute, Executive Order, and/or Presidential Proclamation; Also any other kind of administrative leave such as acts of God (i.e. hurricanes, snow storms, tornadoes, etc.), Presidential funerals, or any other unexpected Government closures.

7 DELIVERABLES AND REPORTING REQUIREMENTS

7.1 Deliverables Table

The contractor is expected to develop and maintain a Program Management Plan (PMP) for the supported task(s). The following schedule of milestones and deliverable submission dates will be used by the Technical Representative and COR to monitor timely progress under this Task Order.

The following abbreviations are used in this schedule:

- N/A: Not Applicable
- i.a.w.: In accordance with
- NLT: No later than
- TOA: Task Order Award
- TR: Technical Representative
- *: Uploaded to GSA ITSS Portal
- All references to days imply calendar days, unless otherwise noted

PWS Ref	Title	Distribution	Delivery Date
Appendix T	Non-Disclosure Agreement	COR	Signed statements are due, from each employee assigned, *prior to* performing *ANY* work on this task.
4.1 Appendix E	*Senior Management Reviews (SMR) Report	COR, TR	NLT 45 Days Post Award and NLT 15th of each month
4.1	*Transition Plan – Incoming Transition	COR, CO	NLT 5 Days Post Award or at Contract Kick-Off Meeting (whichever is sooner)
4.1	*Transition Plan – Outgoing Transition	COR, CO	NLT 90 days prior to Task Order expiration, or when requested by the COR
4.1, Appendix D	*Quality Control Plan	COR, CO	NLT 10 Days Post Kick-off meeting
4.1	Kick -Off Meeting	COR, CO	NLT 10 Days Post Award
4.1	*Kick-Off Meeting Minutes	COR, CO	NLT 10 Days Post Kick-off meeting

4.1	Orientation Briefing	COR, TR	NLT 14 Days Post Award
4.1	Interim Progress Review	COR, CO, TR	Annual
4.1	Problem Notification Reports	COR, CO, TR	NLT 10 Days After Notification
4.1	*Program Management Plan and Schedule	COR, CO, TR	NLT 5 Days After Project kickoff meeting
4.2	Software requirements specification	COR, TR	NLT 45 Days Post Award, updated upon request
4.2	Release notes	COR, TR	NLT 10 Days prior to any software update/release
4.2	User Guides	COR, TR	NLT 10 Days prior to change in user functionality, updated upon request
4.2	Interface Control Document (ICD)	COR, TR	NLT 10 Days Post interface modification
4.2	Administration Guide for JPAS and DISS	COR, TR	NLT 45 Days Post Award, updated upon request
4.2	Continuity of Operations Plan (COOP) for JPAS and DISS	COR, TR	NLT 45 Days Post Award and NLT 30 Days prior to failover test
4.2	Interface Control Document (ICD) for JPAS and DISS	COR, TR	NLT 10 Days Post interface modification, updated as needed
4.2	Change Requests	COR, TR	NLT 30 Days Post Award, updated as needed
4.2	Problem Reports	COR, TR	NLT 30 Days Post Award, updated as needed
4.3	JPAS Weekly Report	COR, TR	Weekly, NLT 2nd business day of the week
4.3	SWFT Quarterly Newsletter	COR, TR	Quarterly, Initial NLT 100 Days Post Award
4.4	Test Management Plan (TMP) for DCII, SWFT, iIRR, and DISS	COR, TR	NLT 15 Day prior to scheduled testing
4.5, 4.7	Configuration Management (CM) Plan	COR, TR	NLT 30 Days Post Award, updated as needed
4.6	Monthly Vulnerability Analysis Report for JPAS and DISS	COR, TR	Monthly, NLT 15th of each month, initial NLT 45 Days Post Award
4.6	IA Report for JPAS and DISS	COR, TR	Monthly, NLT 15th of each month, initial NLT 45 Days Post Award
4.7	Functional Test Guide	COR	NLT 15 days prior to testing
4.7	*Program Management Plan and Schedule	COR, TR	NLT 5 Days Post Kick-off meeting

4.7	Source code and configuration files	COR, TR	NLT 15 Business Days prior to the scheduled software version test start date, updated as needed
4.7	Executable software libraries	COR, TR	NLT 15 Business Days prior to the scheduled software version test start date, updated as needed
4.7	*Project Plan & Schedule	COR, TR	NLT 5 Days Post Kick-off meeting
4.7	High Level Design (HLD) document, Low Level Design (LLD) document	COR, TR	Initial 30 Days Post Award, as required
10.1.3	Trip Report	COR, TR	NLT 10 Days after Trip if needed

7.2 Deliverables Media

Identified below is the range of electronic deliverable types. The Contractor shall submit electronic deliverables in a format compatible with current versions of the specified software in use by the client.

- Text – Microsoft Word
- Spreadsheets – Microsoft Excel
- Briefings – Microsoft PowerPoint
- Drawings – Microsoft Visio
- Schedules – Microsoft Project

Other file formats (example: .pdf) may be acceptable as mutually agreed and coordinated with the COR.

7.3 Basis of Acceptance

The basis for acceptance shall be compliance with the requirements set forth in the Task Order, the Contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with applicable clauses.

Deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables.

7.4 General Acceptance Criteria

Deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this task order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government as specified herein.
- File Editing – All text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow Army guidance. Where none exists, the Contractor shall coordinate approval of format with the COR.
- Timeliness – Deliverables shall be submitted on or before the due date specified.

For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction or other mutually agreeable methods.

7.5 Draft Deliverables

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version. All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling/grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the COR.

7.6 Written Acceptance/Rejection of Deliverables by the Government

The Government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) work days from Government receipt of the draft deliverable.

Upon receipt of the Government comments, the Contractor shall have ten (10) work days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form. The Government shall provide written notification of acceptance or rejection of all final deliverables within fifteen (15) work days. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

7.7 Non-Conforming Products or Services

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the Contractor, within ten (10) work days of the rejection notice. If the deficiencies cannot be corrected within ten (10) work days, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) work days.

8 CONTRACTOR PERSONNEL REQUIREMENTS

8.1 Key Personnel Requirements

The following labor categories are considered key personnel by the Government:

- Program Manager
- Senior Systems Engineer
- Database Administrator/Manager
- Senior Test Engineer

A key person is someone who is integral and indispensable in completing this task order. Key personnel shall be available at project start. The Government requires that at least one Key Personnel be identified as the primary point of contact for this task order. The contractor shall comply with applicable provisions of the ALLIANT GWAC regarding key personnel and personnel substitutions. Additionally, the contractor shall comply with the following:

a. The contractor shall notify the GSA COR and DMDC COR at least ten (10) calendar days before making changes in task personnel.
b. The contractor shall provide a replacement resume to the GSA COR and DMDC COR at the time of notification. Personnel shall be of equal or superior qualifications as the individual being replaced.
c. The resume must be approved by the Government prior to assignment of the replacement personnel to this task order.

One person on the contractor staff shall be the Task Order Manager, a key personnel, and be the Government's technical point of contact for this task order.

8.2 Identification of Contractor Employees

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace are with their name and company/contractor affiliation.

8.3 Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

8.4 Unauthorized Disclosure

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases. If either the Government or the Contractor discovers new or unanticipated threats or hazards, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

8.5 Contractor Interfaces

The Contractor and/or its subcontractors may be required as part of the performance of this effort to work with other Contractors working for the Government. Such other Contractors shall not direct this Contractor and/or their subcontractors in any manner. Also, this Contractor and/or their subcontractors shall not direct the work of other Contractors in any manner. The Government shall establish an initial contact between the Contractor and other Contractors and shall participate in an initial meeting. Any Contracting Officer's Representatives (COR) of other efforts shall be included in an initial meeting.

8.6 Remote Access

Contractor will use DMDC's remote access network infrastructure. The contractor will furnish:

- Stable, high-quality Internet Bandwidth
- Non-GFE workstations capable of installing and executing hardware and software necessary to use VPN remote access tools for network authentication and access control points. Non-GFE workstations shall include standard peripheral devices required for complete functionality (i.e., monitor, keyboard, mouse, etc.). In addition, the contractor shall provide the following additional peripheral devices: Common Access Card (smartcard) compatible card reader.
- The contractor shall comply with all information technology security requirements. For Non-GFE workstations capable of access the DMDC network, the contractor shall maintain patch levels in compliance with the DoD's IAVA program; maintain antivirus updates; and, maintain DMDC mandated software configurations.
- The contractor shall, when security incidents are detected regardless of the source of the incident, promptly notify the DMDC help desk as well as immediately discontinuing the use of workstations. If malware is the source of the security incident, the contractor shall promptly eradicate the malware.
- Non-secure Telephone, facsimile, and voicemail capabilities.

The Government shall provide VPN remote access tools as GFE. Non-GFE workstations shall be capable of installing and executing the following software configurations (VPN access tools): Cisco VPN client; Microsoft Windows Terminal Service client; ActivClient 6 or newer; and Antivirus DoD approved vendor & version.

Remote access is controlled via a Common Access Card (CAC)-enabled to access Virtual Private Network (VPN). The contractor shall ensure that only those personnel having a compelling operational need will request such access and shall keep this number to the absolute minimum necessary to accomplish the mission. This access will be granted to personnel only via an approved System Access Request (SAR). Access will only be granted from the contractor's or DMDC's network. This subnet will conform to DoD Directive 8500.1, DoD Instruction 8500.2, and appropriate Security Technical Implementation Guides, including, but not limited to, Secure Remote Computing, Enclave Security, and Network Infrastructure. The subnet will require accreditation by the DMDC Designated Accrediting Authority (DAA) under the Certification and Accreditation Process. The contractor shall assist with the implementation of the Certification and Accreditation on this subnet.

9 SECURITY

The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Information Assurance (IA), DoD Instruction 8500.2 Information Assurance (IA) Implementation, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoD 8500.1 and DoDI 8500.2 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to the Certification and Accreditation process and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to the Certification and Accreditation process must present evidence of Certification and Accreditation (C&A) testing in the form System Identification Profile (SIP), Certification and Accreditation Implementation Plan, Certification and Accreditation Scorecard, and Plan of Action and Milestones (POA&M). Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of IA C&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

Prior to beginning work on this contract, all Contractor personnel with access to or responsibility for nonpublic Government data under this contract must comply with DODI 5200.2-R, fully adjudicated SSBI, and the Contractor shall ensure that all such personnel are designated as no less than an IT-II or equivalent.

Contractor personnel with access to DoD nonpublic Government data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must:

a. Be CAC or PIV ready prior to reporting for work. At minimum all Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check), two forms of identity proofed identification (I-9 document), and submit a National Agency Check and Law Credit (NACLAC) vetting package for processing. Obtaining CAC or PIV ready status is the responsibility of the contracting agency. It is the responsibility of the contracting agency to notify DMDC when this is complete.
b. Be citizens of the United States.
c. Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication of a NACLAC as required for Federal employment.

If at any time, any Contractor person requiring a CAC is unable to obtain/maintain an adjudicated NACLAC, the Contractor shall immediately notify the DMDC Information Assurance Branch (IA) remove such person from work under this contract.

To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information the Contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The Contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

The Contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract.

Contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the Contracting Officer Representative (COR) and corrective actions will be implemented immediately.

The Contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual's first name or first initial and last name in combination with any one or more of the following data elements including, but not limited to: social security number; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.

The Government may terminate this contract for default if Contractor or an employee of the Contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

The Contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

JPAS and DISS require two personnel with Top Secret/Sensitive Compartmented Information (TS/SCI). One person must be for production support and one person must be for data analysis.

JPAS and DISS require personnel to have a favorably adjudicated Single Scope Background Investigation (SSBI), with a minimum of Secret access.

DCII and iIRR require personnel to have a favorably adjudicated Single Scope Background Investigation (SSBI), with a minimum of Secret access only if the personnel need to access production data; otherwise a Secret eligibility is required.

SWFT requires personnel to have a favorably adjudicated Single Scope Background Investigation (SSBI), with a minimum of Secret access only if the personnel need to access production data; otherwise a Secret eligibility is required.

Government Facility Access - For selected personnel at contract award and in coordination with Technical Point of Contact (TPoC) the contractor shall request and obtain Common Access Cards (CAC) for logical and/or physical access to Government resources. The Contracting Officer's Representative (COR) shall notify the contractor of any increased security requirements, if they occur, and the contractor shall submit adequate clearance packages within 10 calendar days of identification of increased security requirements.

10 OTHER DIRECT COSTS (ODCS)

10.1 Travel

Travel may be required at irregular intervals to the DMDC locations. The Contractor will be reimbursed for travel to provide support at a Government site or other site as may be specified and approved by the COR under this effort. All travel shall be approved, by the COR, prior to commencement of travel. The contractor shall be reimbursed for actual allowable, allocable, and reasonable travel costs, including local travel, incurred during performance of this effort in accordance with the Joint Travel Regulations (JTR) currently in effect on the date of travel.

The task order will establish a ceiling of $50,000.00 each year which cannot be exceeded without the advance approval of the Contracting Officer. No profit or fee shall be added.

Possible travel includes, but is not limited to, the following DMDC locations: DoD Center in Seaside, CA; Mark Center in Alexandria, VA; Iron Mountain in Boyers, PA; DISA Data Center in Columbus, OH.

10.1.1 Use of Government Transportation

The contractor is authorized to use available Government transportation services (Shuttle Buses) and operate and ride in vehicles (Transportation Motor Pool (TMP) to perform mission requirements (per FAR Clause 51.200 Contractor Use of Interagency Fleet Management System (IFMS) Vehicles). The contractor will be required to obtain necessary TMP licensing, training requirements and insurance to operate TMP vehicles. The usage and availability of Government transportation resources will be determined by individual site organizational polices. The COR will determine usage due to availability of Government transportation resources. If Government transportation resources are available to meet mission requirements and the contractor chooses to another form of transportation, the Government will not reimburse the contractor.

10.1.2 Travel Regulations

The Contractor shall adhere to the following travel regulations (see FAR 31.205-46):

- Federal Travel Regulations (FTR) – prescribed by the General Services Administration, for travel in the contiguous United States.
- Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas”, prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

10.1.3 Travel Authorization Requests

Before undertaking travel to any Government site or any other site in performance of this Task Order, the Contractor shall have this travel approved by, and coordinated with, the COR. The Contractor shall notify the COR prior to any anticipated travel. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the Contractor shall prepare a Travel Authorization Request for Government review and approval. The Government shall approve all travel in writing. Long distance travel will be reimbursed for cost of travel comparable with the FTR and DSSR.

Requests for travel approval shall:

- Be prepared in a legible manner;
- Include a description of the travel proposed including a statement as to purpose;
- Be summarized by traveler;
- Identify the travel request/travel authorization number associated with the travel;

- Be submitted in advance of the travel with sufficient time to permit review and approval.
- Not be considered approved until written approval is received from the COR (email shall suffice).

The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

10.1.3 Trip Reports

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

10.2 Non-Travel ODCs/Tools

The Government may require the Contractor to incur ODCs incidental to performance under this task order. Such requirements will be identified at the time the TO is issued or may be identified during the course of the TO, by the Government or the Contractor. Reimbursement will be made as specified in the task order, consistent with the Alliant Contract.

All Non-Travel ODC items (including tools) shall have the written approval of the COR prior to procurement. Federal contracting laws and regulations apply to all Contractor open market purchases of materials and equipment under this task order. Prices must be determined fair and reasonable from competitive sources and are subject to Government audit. The Contractor shall maintain records documenting competitive sourcing, in strict compliance with the competition requirements set forth in the Federal Acquisition Regulation (FAR), for all material and ODC purchases. The Contractor shall provide copies of all such documentation upon request from the Government to verify that the Contractor complied with the competition requirements set forth in the FAR. Within the Contractor's price quote, any such rate shall be identified along with the DCAA point of contact (name, address, phone #, and email address) for rate verification. The Contractor shall only be allowed to apply indirect rates to ODC costs after award if such application is consistent with their successful price proposal and DCAA recommendations. No profit or fee will be allowed on ODC costs.

All ODC items/materials purchased by the Contractor for the use or ownership of the Federal Government will become property of the Federal Government. If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the task order. The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the said hardware/software maintenance support acquired by the Contractor on a cost reimbursable basis.

It is anticipated that miscellaneous ODCs necessary and incidental to performance may include but are not limited to:

- supplies, materials
- printing/copying costs; packaging & marking materials; shipping expenses
- hardware/software
- related IT items

Non-travel ODCs/Tools may be purchased through the Optional Support CLIN if determined to be within the scope of this task order. No profit or fee shall be added.

11 ADMINISTRATIVE CONSIDERATIONS

11.1 Government Furnished Property/Information

The contractor shall assume it will be responsible for providing all resources including all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items necessary to provide the non-personal services detailed herein at the contractor facility. The contractor's environment does not have to mirror the production, pre-production, and failover environments.

NOTE: Development and Contractor Test environments (to include software, hardware, and licenses to support these environments) WILL NOT be provided by DMDC under this task order for JPAS and SWFT. Environments provided for JPAS and SWFT are pre-production, production, failover, and other replicated environments used for reporting.

The only exception is the Government will provide the DISS contractors working on-site at the DMDC Data Center in Seaside, CA with GFP for use (i.e. computer, cubicle, chair, telephone, etc.)

11.2 Points of Contact

Contracting Officer Representative (COR)
Michael Freeman
Defense Manpower Data Center (DMDC)
4800 Mark Center Dr.
Alexandria, VA 22350
571-372-1006
michael.j.freeman.civ@mail.mil

GSA COR / Information Technology Manager
Michael Baumann
IT Specialist, GSA FAS R3
215-446-5852
Michael.baumann@gsa.gov

GSA Contracting Officer
Christine Chaapel
Contracting Officer, GSA FAS R3
215-446-5857
christine.chaapel@gsa.gov

GSA Contract Specialist
Kevin Flynn
Contract Specialist, GSA FAS R3
215-446-5090
kevin.flynn@gsa.gov

11.3 Correspondence

To promote timely and effective administration, correspondence shall be subject to the following procedures:

a. Technical correspondence (where technical issues relating to compliance with the requirements herein) shall be addressed to the Contracting Officer's Representative (COR) with an information copy to the Contracting Officer (CO) and the Contract Administrator (CA).
b. All other correspondence, including invoices, (that which proposes or otherwise involves waivers, deviations or modifications to the requirements, terms or conditions of this PWS) shall be addressed to the Contracting Officer with an information copy to the COR.

12 CLAUSES

12.1 Federal Acquisition Regulation (FAR)

CLAUSE NO.	CLAUSE TITLE	DATE
SECTION 9.5	ORGANIZATIONAL CONFLICT OF INTEREST	
52.203-11	CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	(SEP 2007)
52.204-2	SECURITY REQUIREMENTS	(AUG 1996)
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	(JAN 2011)
52.215-21	REQUIREMENTS FOR COST OR PRICING DATA OR INFORMATION OTHER THAN COST OR PRICING DATA – MODIFICATIONS	(OCT 2010)
52.217-8	OPTION TO EXTEND SERVICES Fill-In Date: 30 days; 60 days; 60 months	(NOV 1999)
52.217-9	OPTION TO EXTEND THE TERM OF THE CONTRACT Fill in Dates: 30 days, 60 days.	(MAR 2000)
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	(JUL 2013)
52.222-25	AFFIRMATIVE ACTION COMPLIANCE	(APR 1984)
52.224-2	PRIVACY ACT NOTIFICATION	(APR 1984)
52.227-14	RIGHTS IN DATA- GENERAL	(DEC 2007)
52.227-21	TECHNICAL DATA DECLARATION REVISION AND WITHHOLDING OF PAYMENT – MAJOR SYSTEMS	(DEC 2007)
52.232-18	AVAILABILITY OF FUNDS	(APR 1984)
52.232-19	AVAILABILITY OF FUNDS FOR NEXT FY	(APR 1984)
52.232-2	LIMITATION OF COST	(APR 1984)
52.232-22	LIMITATION OF FUNDS	(APR 1984)
52.237-3	CONTINUITY OF SERVICES	(JAN 1991)
52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS	(JUL 2013)
52.245-1	GOVERNMENT PROPERTY	(APR 2012)
52.251-1	AUTHORIZATION TO USE GOVERNMENT SUPPLY SOURCES	(APR 2012)
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	(AUG 2013)

52.217-5	EVALUATION OF OPTIONS	(JUL 1990)
52.245-1	GOVERNMENT PROPERTY	(JUN 2007)
52.237-3	CONTINUITY OF SERVICES	(JAN 1991)

12.2 Defense Federal Acquisition Regulation Supplement (DFARS)

CLAUSE NO.	CLAUSE TITLE	DATE
	CONTRACTOR MANPOWER REPORTING	
252.204-7004	ALTERNATE A CENTRAL CONTRACTOR REGISTRATION	(MAY 2013)
252.227-7013	RIGHTS IN TECHNICAL DATA - NONCOMMERCIAL ITEMS	(JUN 2013)
252.227-7014	RIGHTS IN NONCOMMERCIAL COMPUTER SOFTWARE AND NONCOMMERCIAL COMPUTER SOFTWARE DOCUMENTATION	(MAY 2013)
252.227-7015	TECHNICAL DATA- COMMERCIAL ITEMS	(JUN 2013)
252.227-7016	RIGHTS IN BID OR PROPOSAL INFORMATION	(JUN 2011)
252.227-7019	VALIDATION OF ASSERTED RESTRICTIONS - COMPUTER SOFTWARE	(SEP 2011)
252.227-7028	TECHNICAL DATA OR COMPUTER SOFTWARE PREVIOUSLY DELIVERED TO THE GOVERNMENT	(JUN 1995)
252.232-7007	LIMITATION OF GOVERNMENT'S OBLIGATION	(MAY 2006)
252.239-7001	INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION	(JAN 2008)

12.3 Contractor Manpower Reporting

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Defense Manpower Data Center via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year.

Contractors may direct questions to the help desk at: http://www.ecmra.mil.

12.4 Section 508 Compliance

The contractor shall support the Government in its compliance with Section 508 through-out the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities who are members of the public seeking information or services from the Federal Agency, have access to and use of information and data that is comparable to that provided to the pubic who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

The Offeror shall review the following websites for additional 508 compliance information:
http://www.section508.gov/index.cfm?FuseAction=Content&id=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

12.5 Non-Personal Services

As stated in the Federal Register, Volume 57, No. 190, page 45096, dated September 30, 1992, Policy Letter on Inherently Governmental Functions, no personal services shall be performed under this contract. All work requirements shall flow only from the Project Officer to the Contractor's Senior Project Manager. No Contractor employee shall be directly supervised by the Government. The applicable employee supervisor shall give all individual employee assignments, and daily work direction. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently governmental actions under this contract. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government contractors in connection with this contract, the Contractor employee shall state that he/she has no authority to, in any way, change the contract and that if the other contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer. The Contractor shall insure that all of its employees working on this contract are informed of the substance of this article. Nothing in this article shall limit the Government's rights in any way under the other provisions of the contract, including those related to the Government's right to inspect and accept the services

12.6 GSA Region 3 Invoice Clause

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month *(for services)* or
(2) The end of the month in which the products *(commodities)* or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total <u>cumulative</u> hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

For Firm Fixed Price contracts, each month the Contractor shall invoice 1/12th of the overall FFP. Each invoice shall be broken down by the CLIN and sub-CLIN level.

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:
For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.
- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

- If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.
- When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance

Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Contract Number
2. Contract ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COR before payment is processed, *if necessary*.

Close-out Procedures.
General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

13 APPENDICES

Appendix A – Combined Performance Requirements Summary
Appendix B – Guidelines & Parameters for Resolving Systems Problems
Appendix C – System Outage Notification Procedures
Appendix D – Quality Control Plan (QCP)
Appendix E – Senior Management Review (SMR) Template
Appendix F – JPAS Technical Information
Appendix G – DCII Architecture
Appendix H – SWFT Technical Information
Appendix I – EMMA Functional Specifications v4.1
Appendix J – SecurityInfrastructureService_5.0_FunctSpec
Appendix K – Common Update Framework for Developers
Appendix L – CUF Data Access Processors
Appendix M – CUF Subject Processors
Appendix N – Contractor Non-Disclosure Agreement

Appendix O – iIRR Production Environment
Appendix P – Quality Assurance Surveillance Plan
Appendix Q – DMDC Application and Development Process
Appendix R – PSA Interim Quality Assurance Requirements & Processes
Appendix S – Historical PSA Systems Information
Appendix T – DISS Technical Information
Appendix U – DISS Metrics